Expanded Quantum Cryptographic Entangling Probe

Howard E. Brandt
U.S. Army Research Laboratory, Adelphi, MD
hbrandt@arl.army.mil

John M. Myers
Gordon McKay Laboratory, Harvard University, Cambridge, MA
myers@deas.harvard.edu

February 1, 2008

Abstract

The paper [Howard E. Brandt, "Quantum Cryptographic Entangling Probe," Phys. Rev. A **71**, 042312 (2005)] is generalized to include the full range of error rates for the projectively measured quantum cryptographic entangling probe.

Keywords: quantum cryptography, quantum key distribution, quantum communication, entanglement.

PACS: 03.67.Dd, 03.67.Hk, 03.65.Ta

1 INTRODUCTION

Recently, a design was presented [1], [2] for an optimized entangling probe attacking the BB84 Protocol [3] of quantum key distribution (QKD) and yielding maximum Renyi information to the probe for a set error rate induced by the probe. Probe photon polarization states become optimally entangled with the BB84 signal states on their way between the legitimate transmitter and receiver. Standard von Neumann projective measurements of the probe yield maximum information on the pre-privacy amplified key, once basis information is revealed during reconciliation. A simple quantum circuit was found, consisting of a single CNOT gate, and faithfully producing the optimal entanglement. The control qubit consists of two photon polarization-basis states of the signal, the target qubit consists of two probe photon polarization basis states, and the initial state of the probe is set by an explicit algebraic function of the error rate to be induced by the probe. A method was determined for measuring the appropriate probe states correlated with the BB84 signal states and yielding maximum Renyi information to the probe. It was assumed throughout that the error rate

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 FEB 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Expanded Quantum Cryptographic Entangling Probe	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Research Laboratory,Adelphi,MD**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The paper [Howard E. Brandt, "Quantum Cryptographic Entangling Probe," Phys. Rev. A 71, 042312 (2005)] is generalized to include the full range of error rates for the projectively measured quantum cryptographic entangling probe.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**4**	

E induced by the probe in the legitimate signal was such that $0 \leq E \leq 1/4$ for the projectively measured probe. Here we extend the analysis to cover the full range of theoretical interest, namely $0 \leq E \leq 1/3$.

2 GENERALIZED ENTANGLING PROBE

In the present work a generalization is given to include the full range of error rates, $0 \leq E \leq 1/3$. To accomplish this, the following sign choices must be made for the probe parameter μ in Eqs. (26) and (27) of [1]:

$$\cos\mu = [(1+\eta)/2]^{1/2}, \tag{1}$$

$$\sin\mu = \mathrm{sgn}(1-4E)[(1-\eta)/2]^{1/2}, \tag{2}$$

in which we define

$$\mathrm{sgn}(x) \equiv \begin{cases} 1, & x > 0 \\ 0, & x = 0 \\ -1, & x < 0 \end{cases} \tag{3}$$

One also has the definition, Eq. (75) of [1]:

$$\eta \equiv \left[8E(1-2E)\right]^{1/2}. \tag{4}$$

In this case, the probe states $|A_1\rangle$, $|A_2\rangle$, $|\alpha_+\rangle$, $|\alpha_-\rangle$, and $|\alpha\rangle$ of [1] become:

$$|A_1\rangle \equiv \left[\frac{1}{2}(1+\eta)\right]^{1/2} |w_0\rangle + \ \mathrm{sgn}(1-4E)\left[\frac{1}{2}(1-\eta)\right]^{1/2} |w_3\rangle\,, \tag{5}$$

$$|A_2\rangle \equiv \ \mathrm{sgn}(1-4E)\left[\frac{1}{2}(1-\eta)\right]^{1/2} |w_0\rangle + \left[\frac{1}{2}(1+\eta)\right]^{1/2} |w_3\rangle\,, \tag{6}$$

$$\begin{aligned} |\alpha_+\rangle \ = \ & \left[\left(2^{1/2}+1\right)(1+\eta)^{1/2} + \mathrm{sgn}(1-4E)\left(2^{1/2}-1\right)(1-\eta)^{1/2}\right]|w_0\rangle \\ & + \left[\mathrm{sgn}(1-4E)\left(2^{1/2}+1\right)(1-\eta)^{1/2} + \left(2^{1/2}-1\right)(1+\eta)^{1/2}\right]|w_3\rangle\,, \end{aligned} \tag{7}$$

$$\begin{aligned} |\alpha_-\rangle \ = \ & \left[\left(2^{1/2}-1\right)(1+\eta)^{1/2} + \mathrm{sgn}(1-4E)\left(2^{1/2}+1\right)(1-\eta)^{1/2}\right]|w_0\rangle \\ & + \left[\mathrm{sgn}(1-4E)\left(2^{1/2}-1\right)(1-\eta)^{1/2} + \left(2^{1/2}+1\right)(1+\eta)^{1/2}\right]|w_3\rangle\,, \end{aligned} \tag{8}$$

$$\begin{aligned} |\alpha\rangle \ = \ & \left[\mathrm{sgn}(1-4E)\,(1-\eta)^{1/2} - (1+\eta)^{1/2}\right]|w_0\rangle \\ & + \left[(1+\eta)^{1/2} - \mathrm{sgn}(1-4E)\,(1-\eta)^{1/2}\right]|w_3\rangle\,, \end{aligned} \tag{9}$$

respectively, where $|w_0\rangle$ and $|w_3\rangle$ are the orthonormal basis states in the two-dimensional Hilbert space of the probe. As in [1], the upper sign choice in Eq. (23) of [1] has been chosen. Note that Eqs. (5)-(9) are consistent with Eqs. (207), (210), (204), (205), and (74) of [1] for $0 \leq E \leq 1/4$, as must be the case. It then follows that Eq. (71) of [1], along with Eqs. (7)-(9) above, now apply for $0 \leq E \leq 1/3$. (Note that $E = 1/3$ corresponds to complete information gain by the quantum cryptographic entangling probe.) Also the probe and measurement implementations remain the same (as in [1], [2]) with the initial state of the probe now given by Eq. (6). In obtaining the maximum Renyi information gain I^R_{opt} by the probe, Eq. (208) of [1], from Eqs. (7) and (8) above and Eqs. (23) and (17) of [4] and the discussion following Eq. (75) of [1], one first has

$$I^R_{opt} = \log_2(2 - Q^2), \tag{10}$$

and one readily obtains for the overlap Q of correlated probe states:

$$Q = \frac{\langle \alpha_+ | \alpha_- \rangle}{|\alpha_+||\alpha_-|} = \frac{1 + 3\mathrm{sgn}(1-4E)(1-\eta^2)^{1/2}}{3 + \mathrm{sgn}(1-4E)(1-\eta^2)^{1/2}}. \tag{11}$$

Then substituting Eq. (4) in Eq. (11), one obtains

$$Q = \frac{1 + 3\mathrm{sgn}(1-4E)((1-4E)^2)^{1/2}}{3 + \mathrm{sgn}(1-4E)((1-4E)^2)^{1/2}}, \tag{12}$$

where we mean the positive square root; i.e.

$$((1-4E)^2)^{1/2} = |1-4E|. \tag{13}$$

On noting that

$$\mathrm{sgn}(1-4E)|1-4E| = 1-4E, \tag{14}$$

and substituting Eqs. (13) and (14) in Eq. (12), one obtains

$$Q = \frac{1-3E}{1-E}. \tag{15}$$

Finally, substituting Eq. (15) in Eq. (10), one obtains Eq. (208) of [1] , namely,

$$I^R_{opt} = \log_2 \left[2 - \left(\frac{1-3E}{1-E} \right)^2 \right], \tag{16}$$

for the full range of error rates, $0 \leq E \leq 1/3$, as required.

3 CONCLUSION

The quantum cryptographic entangling probe defined in [1], [2] has been generalized to include the full range of error rates, $0 \leq E \leq 1/3$, induced by the probe.

4 ACKNOWLEDGEMENTS

This work was supported by the U.S. Army Research Laboratory and the Defense Advanced Research Projects Agency.

References

[1] H. E. Brandt, "Quantum-cryptographic entangling probe," Phys. Rev. A **71**, 042312(14) (2005).

[2] H. E. Brandt, "Design for a quantum cryptographic entangling probe," to appear in J. Mod. Optics (2005).

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175–179.

[4] H. E. Brandt, "Probe optimization in four-state protocol of quantum cryptography," Phys. Rev. A **66**, 032303(16) (2002).